PRIVACY ACT REVIEW

SUBMISSION

AISA

AUSTRALIAN INFORMATION SECURITY ASSOCIATION

COVERING LETTER

10.1.2022

Attorney-General's Department
4 National Circuit BARTON ACT 2600
By email: PrivacyActReview@ag.gov.au

Dear Attorney-General,

RE: Australian Information Security Association Submission to the Privacy Act Review – Discussion Paper (October 2021).

We have attached a submission on the Privacy Act Review from our perspective as the peak professional body for information security and cyber security in the region.

We have no objection to the publication of this submission, and no redactions are required prior to publication.

Thank you for the opportunity to contribute our views. Please do not hesitate to contact Nicole Stephensen, Michael Trovato or me if you would like clarification of any of the comments made in this submission.

Sincerely,

Damien Manuel
Chairperson, AISA

Email: damien.manuel@aisa.org.au
Mobile: +61 439 319 603

EXECUTIVE SUMMARY

The Australian Information Security Association (AISA) champions the development of a robust information security and privacy sector by building the capacity of professionals and advancing the cyber security and safety of the Australian public as well as businesses and governments in Australia. We welcome the Attorney General's request for submissions in response to the October 2021 Discussion Paper that canvases options and poses key questions for modernising Australia's *Privacy Act 1988.*

Established in 1999 as a nationally recognised and independent not-for-profit organisation and charity, AISA has become the recognised authority and industry body for information security, cyber security and security-related privacy matters in Australia. AISA caters to all domains of the information security industry with a particular focus on sharing expertise from the field at meetings, focus groups and networking opportunities around Australia.

AISA's vision is a world where all people, businesses and governments are educated about the risks and dangers of invasion of privacy, cyber-attack, and data theft and to enable them to take all reasonable precautions to protect themselves. AISA was created to provide leadership for the development, promotion, and improvement of our profession, and AISA's strategic plan calls for continued work in the areas of advocacy, diversity, education, and organisational excellence.

This submission represents the collective views of over 7,500 cyber security, information technology and privacy professionals, allied professionals in industries such as the legal, regulatory, financial, and prudential sector, as well as cyber and IT enthusiasts and students around Australia. AISA members are tasked with protecting and securing public and private sector organisations including national, state and local governments, ASX listed companies, large enterprises, NGO's as well as SME/SMBs across all industries, verticals and sectors.

AISA proactively works to achieve its mission along with its strategic partners. These include the Australian Cyber Security Centre, AustCyber, Cyrise, the Risk Management Institute of Australia (RMIA), the Australian Strategic Policy Institute (ASPI), the Australian Institute of Company Directors (AICD), the Oceania Cyber Security Centre (OCSC), the Australian Security Industry Association Limited (ASIAL) as well as international partner associations such as (ISC)^2, ISACA and the Association of Information Security Professionals (AISP). AISA also works closely with both federal and state / territory governments to ensure a robust and safe sector.

In this submission we have covered matters of particular interest to AISA at this stage of the privacy reform agenda, noting that our 2021 Issues Paper submission canvased at length many of the themes mapped into the present Discussion Paper. AISA has reviewed the submissions of the Office of Australian Information Commissioner (OAIC), Salinger Privacy, Data Synergies and IIS Partners (submitted jointly with Ground Up Consulting). It is AISA's hope that our views will be considered alongside those of our esteemed colleagues, as collectively we are working to ensure enhancements to Australian privacy law improve organisational privacy practice, empower consumers, and protect their data.

TABLE OF CONTENTS

Definition of personal information

Security professionals globally are tasked with preserving the confidentiality, availability, integrity and privacy of all data, of which personal information is a significant subset. Taking account of the various names and associated definitions for 'personal information' found across the range of standards, guidelines and frameworks to which security professionals refer – confidential information, personal information, personal data and personally identifying information (PII), to name a few – there can be confusion in the Australian setting as to the extent of the information we are tasked with protecting.

AISA welcomes the revision of the definition of personal information as proposed in 2.1 – 2.3 of the Discussion Paper. Having reviewed the submissions of our privacy colleagues, who are tasked with supporting good decision-making in relation to privacy beyond matters of security, data breach management and transborder data flows, and also being cognizant of how technology, e-government initiatives, online platforms and services are shaping the privacy landscape, we submit that careful drafting tweaks to achieve greater definitional clarity are required. We support adoption of the drafting changes to the definition of personal information proposed by Salinger Privacy on page 14 of their 03.1.2022 submission.

As a matter of general comment, AISA considers the use of the term 'PII' to describe personal information as ill-advised in the Australian information security sector. We believe that 'protection of PII' is wordplay used largely in the vendor market as a reassuring descriptor of products and services where personal information (and the security of it through its lifecycle) is at issue. However, from the perspective of compliance with Australian privacy rules the reference to PII can result in contractual provisions – as well as physical, technical and other administrative controls (such as policies and procedures) – that fall short of what is required in this region. AISA supports education of the sector and the public in relation to consistent use of the correct definition in Australian settings.

Flexibility of the APPs in regulating and protecting privacy

AISA notes that the APPs, in their current iteration, provide a decision-making framework that should make clear to government and organisations that every piece of personal information collected must be reasonably secured for its lifetime. However, the digital economy and the overwhelming appetite for data (which may – depending on the nature and relative privacy maturity of an organisation – not be viewed as inclusive of the subset of personal information), has undermined the efficacy of key principles of privacy protection: *purpose specification* and *collection limitation*.

The Discussion Paper deals with this to some extent in its proposals at 3.1 – 3.2 regarding the making of APP Codes, where presumably a Code could be used as a vehicle to explicitly require purpose specification and collection limitation in specific contexts (for example, trialling of AI-supported decision-making that uses facial recognition or other data harvesting technologies). If this is the case, then AISA considers this a welcome development.

Likewise, AISA considers the proposals at 8.4 - 8.5 about uplift in respect of privacy notice (aka: collection notice) to potentially have the effect of limiting collections of personal information to those which can be justified in a digestible notice to the individual. We caution, however, that a traditional written privacy notice sufficient for analogue collections (e.g., face-to-face, paper-based forms) may not make sense in all digital contexts. For example, some collections happen while a person is 'in transit' online, where they may submit additional information in relation to a purchase when prompted at the payment gateway (everything from 'add a last minute delivery instruction', to 'pen a personal note to the recipient', or 'give us your mobile number so we can give you updates on your purchase') where the collection is ostensibly new but could disrupt the individual's experience of the service if a privacy notice were to be delivered in the traditional (read: paragraphs on paper) way. We support that any guidelines issued by the OAIC in relation to this aspect of reform should include examples of what good collection notices look like in a cross section of digital and analogue spaces.

AISA supports adoption of proposal 10.4 with respect to making the purposes of collection abundantly clear.

Exemptions

AISA broadly supports removal of the Small Business, Employee Records, Political Acts and Practices and Journalism exemptions from the Privacy Act.

We particularly support removal of the Small Business exemption, as this sector is growing exponentially as an information security and cyber security risk surface. As an example, since the onset of the COVID-19 pandemic many small businesses that directly service the community have altered their business models in order to remain afloat, including the introduction of online sales and services (everything from click-and-collect shopping options, to delivery of food and medicines, to using QR menu codes to replace restaurant table service). Many also are using social media marketplaces and profile pages to interact with customers. In the rush to move online, attention to privacy and security has been scant in most cases and the threats posed by using off-the-shelf contracts with managed service providers, poor authentication methods, phishing and other forms of cyber-attack have largely remained unaddressed in this sector.

It is a matter of urgency that the small businesses currently exempt from Australia's privacy regime be brought meaningfully into the fold. Noting that there will be varying levels of resourcing and business sophistication on the topic of privacy, AISA supports that removal of the Small Business Exemption to include a readiness period for small businesses of at least 18 months and an adequate budget for the OAIC in respect of anticipated training and advisory outputs (during the readiness period) and extending to complaints management (following the readiness period). The OAIC needs to also recognise the type, frequency and tone of messaging to small businesses will require well-funded education and awareness campaigns to drive long lasting and significant behavioural change.

AISA further believes that the efforts of the Australian Cyber Security Centre (ACSC) should be supported with adequate budget to support Small to Medium businesses (SMEs). https://www.cyber.gov.au/acsc/small-and-medium-businesses . It cannot be understated that messaging and communications with the SME sector needs to resonate with the time poor nature of that sector and delivery partners such as AISA, AICD, CPA Australia should be engaged to assist. It is also important to recognise that a one size fits all strategy of communication does not work across SMEs and messaging should be tuned to several business personas (e.g., sole traders, micro businesses etc..).

Security of personal information

Information security – whether in relation to boots on the ground or data in the cloud – is within the direct purview of AISA and its stakeholders. Although APP 11 requires that APP entities take such steps as are reasonable in the circumstances, our experience is that government and organisations alike struggle to understand what the Privacy Act intends as 'reasonable.'

AISA believes that similar to the 'security principle' in the European Union's GDPR, more needs to be done to set the bar for organisations and to achieve the desired privacy outcomes. These should be further defined and specified - if not on the basis of 'targets', then at least on the basis of ameliorating known privacy harms. This should include alignment to international and Australian standards, as appropriate.

AISA supports adoption of proposals 19.1 – 19.2 in respect of clarifying what 'reasonable steps' to secure personal information means in practice and including factors (such as the likelihood of a known privacy harm) in assessment of what is reasonable in the circumstance.

AISA strenuously recommends adoption of proposal 19.3 in relation to the taking of all reasonable steps to destroy or de-identify personal information when it is no longer needed for any purpose and considers this proposal to be consistent with privacy (and security!) best practice globally.

Notifiable Data Breaches Scheme

As noted in our 2021 response to the Issues Paper on this topic, AISA believes compliance with the NDB Scheme is a complex and complicated business problem for government and organisations and requires skill and subject matter expertise to provide guidance. Organisations often ask AISA which requirements they should follow. As such anything that provides clarity (such as additional OAIC guidance) is desired and will be beneficial, both for improving organisational competence and reducing costs of compliance over time.

AISA supports adoption of the proposal at 27.1 that government and organisations take, and be able to articulate in writing that they have taken, steps to contain, investigate, respond to and mitigate privacy harms associated with the unauthorised access to, disclosure or loss of personal information.

AISA also supports OAIC funding for more case studies and online learning modules based on the types of NDBs that have been reported so people can use them to learn what not to do or what to improve. Ideally this will bring to life the statistics on the OAIC website to highlight possible cyber security hygiene issues, issues with misconfiguration of systems, control failures, human errors, and the like.

Conclusion

We thank the Attorney-General for the opportunity to contribute to the phase of privacy law reform in Australia and would be pleased to discuss any aspect of our submission.

If you have any questions or need additional information, please do not hesitate to contact us.

About the Lead Author

Nicole Stephensen, FAISA SCCISP – Director and Principal, Ground Up Consulting

Nicole Stephensen directs Ground Up Consulting Pty Ltd and, as a trusted privacy services partner, has provided Principal Consultant services to IIS Partners since 2017. She provides capacity building and privacy by design services to diverse clientele across all three levels of government, information technology and not-for-profit sectors. With over 20 years in the privacy profession, Nicole believes in building organisational capacity around privacy and embedding best practice into organisational culture.

She has deep public sector privacy expertise, particularly within the privacy regulatory and public policy arenas. Notably, Nicole was asked by the Queensland Department of the Premier and Cabinet to conduct public policy research into and provide drafting instructions for Queensland's first privacy law, the *Information Privacy Act 2009*. She also created and managed the Complaints Management education program at the Queensland Office of the Ombudsman and, while at the Department of Justice at Attorney-General (Queensland's 'lead privacy agency'), was responsible for implementation of the state's early administrative privacy regime under Information Standards 42 and 42A. She has worked for the British Columbia and Alberta privacy regulators and held a principal advisory role at the Queensland Office of the Information Commissioner.

Nicole is a Fellow of AISA (FAISA) and is a recognised leader in privacy acculturation amongst security professionals. She is also a leading member of the International Association of Privacy Professionals (IAPP) and hosts the IAPP's KnowledgeNet Chapter for Queensland. Prior to its incorporation into the larger IAPP in 2019, Nicole was a founding member of the International Association of Privacy Professionals ANZ Chapter (iappANZ) where she sat for three consecutive terms on the Board.

Nicole was the 2020 Smart Cities Council Australia-New Zealand (SCCANZ) Leaderhip Award winner for privacy advocacy and her work building privacy programs for Australian local governments. She is also an Advisory Board member for the SCCANZ Centre for Data Leadership. Nicole held the pro bono position of Executive Director for Privacy and Data Protection at the Internet of Things Security Institute (IoTSI) from its inception until mid-2020 and holds their Smart Cities and Critical Infrastrucure Security Professional (SCCISP) designation.

She is a sought-after international speaker about privacy and the interface between Privacy, Information Security, Risk Management, Ethics and Trust. She is a subject matter expert and Guest Lecturer for the Ducere Global Business School/ University of New England, Queensland University of Technology and the newly-formed Canadian Criminal Justice Academy.

A dual Canadian-Australian citizen, Nicole has lived and worked in Australia since 2003. She holds a Bachelor of Arts (Political Science) degree from the University of Victoria, British Columbia, Canada.

About Contributors

AISA acknowledges the significant contribution of the following individuals in this submission:

Mr Michael Trovato – Board Member, AISA, Managing Director & Lead Security Advisor, IIS Partners

Mike Trovato joined IIS in 2018 with over 40 years' experience in consulting and financial services in Australia, Asia Pacific, and the USA. He is a cyber security, privacy and technology risk advisor to boards, board risk committees, and executive management.

Mike focuses on assisting key stakeholders with understanding the obligations and outcomes of effective privacy and cyber security. This includes solving an organisation's issues with respect to regulatory, industry, and company policy compliance and to protect what matters most in terms of availability, loss of value, regulatory sanctions, or brand and reputation impacts balanced with investment.

At IIS, Mike has led over 100 privacy and security governance, risk, and compliance client engagements across government, health care, education, retail, financial services, and technology sectors. He has also advised clients about the direct impact of cyber security on privacy and data protection and how to provide greater resilience to assure better organisational outcomes.

Mike also serves as ICG's Global Cyber Practice Leader and IIS is an ICG Affiliate. Prior to joining IIS, he was the Founder and Managing Partner of Cyber Risk Advisors. Before then, he was Asia Pacific, Oceania and FSO Lead Partner EY Cyber Security; GM Technology Risk and Security for NAB Group; a Partner within Information Risk Management at KPMG in New York; and has held financial services industry roles at Salomon Brothers and Mastercard International. At EY, Mike was responsible for creating the largest, sustained "Big-4" cyber security practice, deploying Privacy and Data Protection solutions, and building the Melbourne Advanced Security Centre (ASC), specialised in attack and penetration testing.

As the NAB's first Group Technology Risk and Security GM, Mike was responsible for risk assessment, strategy, and the security program with a budget of AU$6 million, 11 direct reports and 40+ team members. He focused on enhancing technology risk and security governance, functional security analysis capabilities, and establishing key regulatory and compliance activities.

Mike is a Graduate of the Australian Institute of Company Directors (GAICD), Member Australian Information Security Association (MAISA), an AISA Board Member, ISACA Melbourne Chapter Board Member, Member of National Standing Committee on Digital Trade.

Mike's professional credentials include being a Certified Information Systems Manager (CISM); Certified Data Privacy Solutions Engineer (CDPSE); and Certified Information Systems Auditor (CISA). He is also a member of the International Association of Privacy Professionals (IAPP) and is an ICG Accredited Professional. He has an MBA, Accounting and Finance and BS, Management Science, Computer Science, and Psychology.

Mike is the co-author of The New Governance of Data and Privacy: Moving from compliance to performance, Australian Institute of Company Directors, November 2018.

Damien Manuel – Chairperson, AISA

As an experienced, results-driven ICT business professional, Damien Manuel has more than 25 years of experience specialising in cyber security, business governance, compliance and risk management.

Damien is the Chairperson of the Australian Information Security Association (AISA), a not-for profit organisation which aims to improve Cyber Security in Australia at a Government, Industry and Community level. Damien also provides advice to several boards both in Australia and internationally. He is a well-known leader in the Australian cyber security sector and works closely with both federal and state / territory governments.

Having recently completed his role at Deakin University as Industry Professor and Director of the Centre for Cyber Security Research & Innovation (CSRI), Damien continues to support the university through his honorary role as Adjunct Professor.

In his former role as the Chief Information Security Officer (CISO) for Symantec Australia and New Zealand, Damien worked with senior executives in the region to align security architectures to industry best practices. He also worked as a senior information security governance manager and later as an enterprise IT and security risk manager at National Australia Bank (NAB), where he was responsible for managing the bank's information security standard globally. He also held senior roles at RSA, Telstra and Melbourne IT and is currently on CompTIA's Executive Advisory Committee.

Damien has supported CompTIA for over 14 years through the development of CompTIA Server+, CompTIA Network+, CompTIA Security+ and more recently the CompTIA Advanced Security Practitioner certification.

Damien's passion for making a difference motivated him to establish Information Technology community resource centres to improve literacy and skills in impoverished and disadvantaged communities in Kenya, Laos, Uganda and Cambodia.

Underpinning his experience is a diverse educational grounding ranging from the highest security, audit and governance certifications complemented by an Executive MBA with an international business focus.